INVERS MATRIKS KUNCI PADA ALGORITMA CHIPER HILL

Berny Pebo Tomasouw
(Sabtu, 22 Februari 2014)

A. PENGANTAR

Misalkan P adalah sebuah pesan (pesan asli a.k.a *plaintext*) yang ingin dirubah menjadi sandi (*chipertext*) C. Algoritma Chiper Hill bekerja dengan cara memilih matriks kunci K yang berukuran $n \times n$ sehingga

$$KP = C$$

Untuk merubah kembali sandi C ke pesan asli maka, kita harus menghitung invers matriks K sehingga bisa diperoleh

$$K^{-1}C = P$$

Dalam penulisan kali ini, saya akan membahas tentang bagaimana cara menghitung invers matriks kunci K^{-1} yang digunakan dalam algoritma Chiper Hill.

B. PEMBAHASAN

Saya akan mulai dengan contoh dari algoritma Chiper Hill sederhana. Misalkan setiap huruf diwakili oleh angka satu sampai 25 , yakni

A = 1,	B = 2,	C = 3,	J = 10,	K = 11,	L = 12,	S = 19,	T = 20,	U = 21,
D = 4,	E = 5,	F = 6,	M = 13,	N = 14,	O = 15,	V = 22,	W = 23,	X = 24,
G = 7,	H = 8,	I = 9,	P = 16,	Q = 17,	R = 18,	Y = 25,	Z = 0.	

Perhatikan bahwa untuk huruf Z tidak menggunakan angka 26, namun menggunakan angka 0 (nol). Selanjutnya, konsep yang akan dipakai adalah konsep modulo. Oleh karena itu, saya akan memberikan sedikit gambaran tentang modulo.

Definisi 1

Misalkan m adalah bilangan bulat. Untuk $a, b \in \mathbb{Z}$ dapat ditulis

$$a \equiv b \pmod{m}$$

dan dibaca "a kongruen dengan b modulo m" jika berlaku $m \mid (a-b)$.

Agar lebih jelas, perhatikan contoh berikut

Contoh 1

a. $18 \equiv 4 \pmod{7}$ karena $18-4=14$ dan 7 membagi 14, yakni $7 \mid 14$.
b. $-22 \equiv 3 \pmod{5}$ karena $-22-3=-25$ dan 5 membagi -25, yakni $5 \mid -25$.
c. Saya ingin mencari bilangan bulat positif yang kongruen dengan -16 mod 7. Yang harus dilakukan adalah menambahkan -16 dengan kelipatan 7 sehingga diperoleh bilangan bulat positif. Diproleh

$$-16+21=5 \text{ sehingga dapat ditulis } -16 \equiv 5 \pmod{7}.$$

Dari contoh di atas saya dapat bentuk notasi baru sebagai berikut

$$\text{mod}(18,7)=4 \;;\quad \text{mod}(-22,5)=3 \quad;\quad \text{mod}(-16,7)=5.$$

Berikutnya, karena akan dihitung invers matriks maka saya akan perlihatkan definsi untuk invers modulo.

Definisi 2

Diberikan $a \in \mathbb{Z}$. Bilangan a^{-1} adalah invers dari a modulo m jika memenuhi

$$a\,a^{-1} = 1 \pmod{m} \text{ atau } a^{-1}a = 1 \pmod{m}$$

Agar lebih jelas, perhatikan contoh berikut

Contoh 2

Saya akan tinjau kasus modulo 26.

a. Invers modulo dari bilangan 7 adalah 15 karena

$$7 \cdot 15 = 105 \text{ dan } 105 \equiv 1 \pmod{26}.$$

b. Invers modulo dari bilangan 11 adalah 19 karena

$$11 \cdot 19 = 209 \text{ dan } \mathrm{mod}(209, 26) = 1.$$

Sampai di sini, saya rasa sudah cukup untuk konsep modulo sehingga saya bisa kembali fokus untuk mencari invers dari matriks kunci. Saya akan meninjau dua kasus, yakni kasus matriks berorde 2×2 dan matriks berorde 3×3.

Contoh 3

Misalkan pesan asli adalah "OR". Saya akan merubah pesan ini menjadi sandi menggunakan Chiper Hill. Matriks kunci yang saya pilih adalah $K = \begin{bmatrix} 8 & 5 \\ 1 & 3 \end{bmatrix}$. Pesan "OR" dirubah menjadi matriks $P = \begin{bmatrix} 15 \\ 18 \end{bmatrix}$ (bisa dilihat kembali angka yang mewakili setiap huruf). Sehingga diperoleh : $KP = \begin{bmatrix} 8 & 5 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 15 \\ 18 \end{bmatrix} = \begin{bmatrix} 210 \\ 69 \end{bmatrix}$. Hitung modulo 26 dari hasli tersebut diperoleh $\begin{bmatrix} 210 \\ 69 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 17 \end{bmatrix} \pmod{26}$. Matriks sandi adalah $C = \begin{bmatrix} 2 \\ 17 \end{bmatrix}$ dan dikonversikan menjadi "BQ".

Untuk mengembalikan sandi "BQ" menjadi pesan asli maka saya harus menghitung invers modulo dari matriks kunci. Cara menghitungnya sebagai berikut :

i. Hitung determinan dari matriks K, diperoleh $\det(K) = 19$.

ii. Hitung adjoin dari matriks K, diperoleh

$$\text{adjoin } K = \begin{bmatrix} 3 & -5 \\ -1 & 8 \end{bmatrix}$$

iii. Untuk modulo 26, invers dari 19 adalah 11, karena $(19 \cdot 11) \equiv 1 \pmod{26}$. Selanjutnya kalikan dengan matriks adjoin dari K, diperoleh

$$11\begin{bmatrix} 3 & -5 \\ -1 & 8 \end{bmatrix} \equiv \begin{bmatrix} 33 & -55 \\ -11 & 88 \end{bmatrix}$$

iv. Dari hasil terakhir, maka bisa dihitung modulo 26 , diperoleh

$$\begin{bmatrix} 33 & -55 \\ -11 & 88 \end{bmatrix} \equiv \begin{bmatrix} 7 & 23 \\ 15 & 10 \end{bmatrix} \pmod{26}$$

Jad invers modulo dari matriks kunci K adalah $K^{-1} = \begin{bmatrix} 7 & 23 \\ 15 & 10 \end{bmatrix}$.

Untuk mendapatkan pesan asli maka saya akan kalikan K^{-1} dengan matriks sandi C yang telah diperoleh sebelumnya, diperoleh

$$\begin{aligned} K^{-1}C &= \begin{bmatrix} 7 & 23 \\ 15 & 10 \end{bmatrix}\begin{bmatrix} 2 \\ 17 \end{bmatrix} \\ &= \begin{bmatrix} 405 \\ 200 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 18 \end{bmatrix} \pmod{26} \end{aligned}$$

Jadi diperoleh matriks $P = \begin{bmatrix} 15 \\ 18 \end{bmatrix}$ yang bisa dikonversikan menjadi pesan asli "OR".

Contoh 4

Dalam contoh ini, saya akan langsung memisalkan matriks kunci yang dipakai adalah $K = \begin{bmatrix} 3 & 4 & 2 \\ 7 & 3 & 9 \\ 2 & 8 & 11 \end{bmatrix}$. Berikut ini adalah langkah-langkah untuk menghitung invers modulo matriks kunci tersebut :

i. Hitung determinan dari matriks K , diperoleh $\det(K) = -253$. Selanjutnya, akan dicari invers modulo dari -253.
   $\mathrm{mod}(-253, 26) = 7$ sehingga invers modulnya adalah 15. (lihat Contoh 2 sebelumnya)

ii. Hitung adjoin dari matriks K, diperoleh

$$\text{adjoin } K = \begin{bmatrix} -39 & -28 & 30 \\ -59 & 29 & -13 \\ 50 & -16 & -19 \end{bmatrix}$$

iii. Selanjutnya kalikan 15 dengan matriks adjoin dari K, diperoleh

$$15\begin{bmatrix} -39 & -28 & 30 \\ -59 & 29 & -13 \\ 50 & -16 & -19 \end{bmatrix} = \begin{bmatrix} -585 & -420 & 450 \\ -885 & 435 & -195 \\ 750 & -240 & -285 \end{bmatrix}$$

iv. Dari hasil terakhir, maka bisa dihitung modulo 26 , diperoleh

$$\begin{bmatrix} -585 & -420 & 450 \\ -885 & 435 & -195 \\ 750 & -240 & -285 \end{bmatrix} \equiv \begin{bmatrix} 13 & 22 & 8 \\ 25 & 19 & 13 \\ 22 & 20 & 1 \end{bmatrix} \pmod{26}$$

Jad invers modulo dari matriks kunci K adalah $K^{-1} = \begin{bmatrix} 13 & 22 & 8 \\ 25 & 19 & 13 \\ 22 & 20 & 1 \end{bmatrix}$.

Catatan :

1. Bisa dibuktikan sendiri bahwa berlaku $K\,K^{-1} \equiv I \pmod{26}$, dimana I adalah matriks identitas.
2. Untuk matriks dengan orde lebih dari 3, cara perhitungan invers modulo tetap sama.

C. PENUTUP

Mohon maaf jika terdapat kekurangan ataupun kesalahan. Saran dan kritik dapat dikirim ke email saya : bernypebo@yahoo.co.id